Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 78 (2014) 96 – 101

Procedia Engineering

www.elsevier.com/locate/procedia

Humanitarian Technology: Science, Systems and Global Impact 2014, HumTech2014

Algorithm for source mobile identification and deactivation in SMS triggered improvised explosive devices

Francis Enejo Idachaba*

Covenant University Ota. Ogun State Nigeria

Abstract

Mobile communication technology can be used for the activation of explosive devices from more remote locations using the short messaging system. The platform eliminates the need for the detonator to be near the Improvised Explosive Devices. It eliminates the need for line of sight between the transmitter and the receiver and can also be used to activate multiple IEDs from one location with one message. This paper presents the development of an algorithm for the minimization or delayed activation of suspected SMS triggered explosive device. It will also enable the detection of GSM enabled IEDs before they are activated and the localization of the source mobile for the trigger SMS in real-time with a possibility of stopping the delivery of such suspected SMS trigger messages.

Selection and peer-review under responsibility of the Organizing Committee of HumTech2014

Keywords: Detonation; Explosive devices; Mobile Communication; Short Messaging System

1. Introduction

Mobile communication technology provides a platform for communication between mobile devices located within the coverage area of the base station antennas. To maximize the available frequencies, the geographical area covered by the antenna is broken down into cells where the frequencies are reused depending on the communication technology and the population/ traffic density in those locations. Figure 1 shows the architecture of a mobile communication network. The mobile communication architecture provides a platform that can be utilized for the activation of multiple IEDs located in different geographical location from one source mobile located in another

* Corresponding author.
E-mail address: idachabafe@yahoo.com

Selection and peer-review under responsibility of the Organizing Committee of HumTech2014
doi:10.1016/j.proeng.2014.07.044

location. These mobile devices can be located on different continents thus making the detection and tracking of the trigger/source mobile impossible.

Nomenclature

BTS Base Transceiver Station
SMS Short Message Service
HLR Home Location Register
VLR Visitor Location Register

1.1. Mobile Communication Technology

There are two dominant mobile communication technologies and they have evolved over the years into different generations. These technologies are the Global System of Mobile communication (GSM) and the Code Division Multiple Access (CDMA) systems. This paper focuses on the GSM technology due to it wide spread deployment.

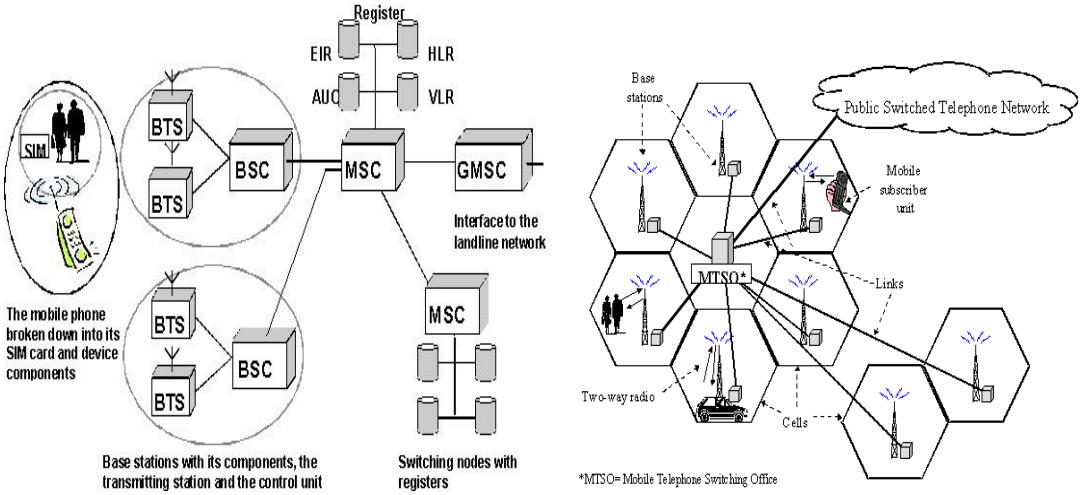

Fig. 1. GSM Mobile Communication Architecture

The GSM architecture consists of a Base Transceiver Station (BTS) connected to a Mobile Switching Center through the Base Station Controller. The details of the mobile unit and the owner details are stored in the HLR and VLR databases while the Gateway MSC (GMSC) provides links to other operator networks.[1][2][3]

1.2. Short Messaging Service

Short Messaging Service (SMS) is a very significant service delivered by mobile communication networks. It involves the transmission of alphanumeric characters (160 characters in length) from a source mobile to a receiving mobile. The SMS can be sent from one mobile to one receiving mobile or from one mobile to multiple receiving mobiles at the same time. The SMS is sent from the originating mobile and it goes through the operator network to the SMS center. An SMS center (SMSC) is responsible for handling the SMS operations of a wireless network. An SMS message may need to pass through more than one network entity (e.g. SMSC and SMS gateway) before reaching the destination. The main duty of an SMSC is to route SMS messages and regulate the process. If the recipient is unavailable or the phone is switched off, the SMSC will store the SMS message. The SMS will be forwarded to the recipient whenever it becomes available. SMSC are usually dedicated to handle the SMS traffic of one wireless network with each operator managing their own but it is possible for a network operator to use a third-

party SMSC that is located outside their wireless network system. The typical SMS network architecture in Figure 2 shows the SMS center and the different databases of the network. These databases are the Home Location Register (HLR) and the Visitor Location Register (VLR). The SMSC uses these data to locate the mobile unit and forwards the messages through the MSC and base station to the destination mobile.

1.2.1. SMS Message Delivery Process

The SMS message delivery process is shown in Figure 3.

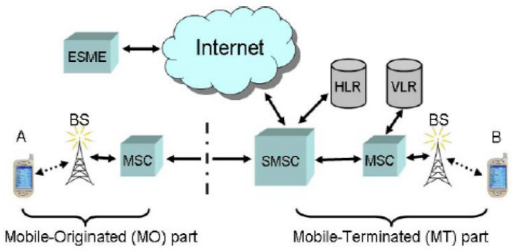

Fig. 2. SMS Architecture

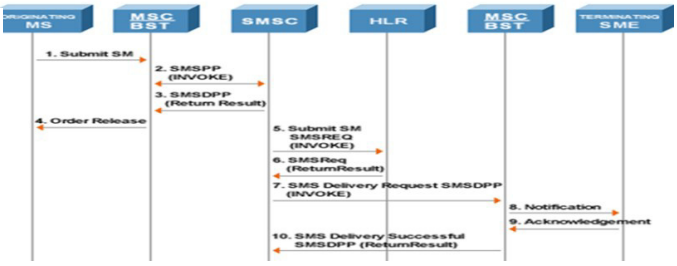

Fig. 3. SMS delivery process

1. The MS transfers the SM to the MSC.
2. The MSC interrogates the home SMSC to verify that the message transfer does not violate the supplementary services invoked or the restrictions imposed. The MSC sends the short message to the home SMSC using the SMSPP Invoke operation
3. The SMSC delivers an acknowledgment to the MSC.
4. The MSC returns order release to the MS.
5. The SMSC queries the HLR for the location of the destination MS.
6. The HLR returns the destination (MSC) serving the destination MS.
7. The SMSC delivers SM to the MSC serving the destination MS.
8. The SMSC delivers the short message to the MS.
9. The MS acknowledges to the MSC the successful outcome of the SMSDPP operation.
10. The MSC returns to the SMSC the outcome of the MO-SM operation (delivery successful)

2. SMS based Control

The combination of the GSM/ Mobile communication technology and the microcontrollers created a new field of remote control where control signals are sent over the communication network in the form of SMS messages. The control messages are received by the receiving mobile and sent to the microcontroller which decodes the messages and activates the relevant switches for controlling the devices[4][5][6][7][8]. A block diagram of this control network is shown in Figure 4.

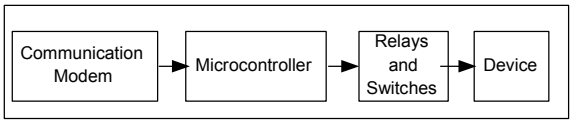

Fig. 4. SMS based remote control architecture

3. Improvised Explosive Devices (IEDs)

IEDs are one of the most destructive terrorist weapons of choice. This is due to the ease of manufacture and the availability of off the shelf materials and electronic components for the design of the trigger systems and the explosive devices [9-16]. Different types of remotely activated IEDs with different characteristics and limitations exist. The cheapest and the most common of these trigger systems require that the remote control be within some distance near the IED. This is to ensure that the trigger signal sent by radio frequency can be received by the IED. The possibility of detecting the trigger source is very high especially in urban areas and cities with multiple cameras. This system also is designed to activate one IED at a time. The use of the mobile communication network and the SMS technology for the delivery of trigger signals make it possible for the trigger source to be located in a different state, country or continent from the IED. This will make it difficult to trace and the multi recipient capability of the SMS technology also enables the delivery of trigger signals to multiple IEDs located in different states as shown in the Figure(s) 5 and 6.

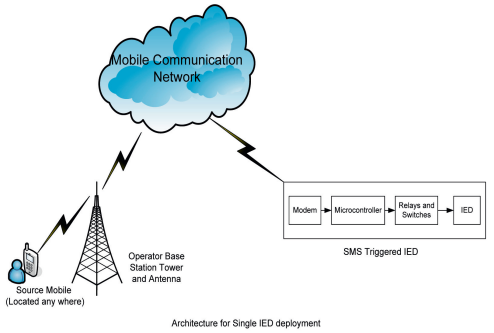

Fig. 5. Architecture for Single IED Deployment

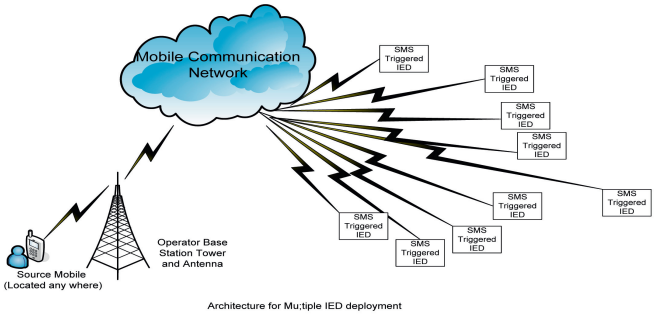

Fig. 6. Architecture for Multiple IED Deployment

4. Algorithm for Source Mobile Identification and Attack Prevention

The objective of the algorithm is to utilize a set of parameters to identify suspicious SMS, delay its delivery and send the details of the originating mobile to relevant security agencies while discarding the message if it is verified to be an IED trigger message. This is achieved without impacting on the network performance and the message delivery time. The algorithm for the identification of a possible trigger is processed by the SMSC and classifies each mobile during the location update sequence. Mobiles that are stationary for several hours and that have no subscriber details at the HLR and no message or call history are classified as suspicious and the locations sent to the security agencies for inspection. The SMSC also monitors the SMS transmissions to recipient mobile units in locations classified as critical either due to the presence of a large number of people (during events) or the presence of a sensitive public infrastructure.

The algorithm is listed below:

1. A list of all the critical areas and the BTS/Sector antenna covering those areas is created in the operator HLR and VLR database.
2. Any location around which there will be a high concentration of people and areas where the security agencies feel there will be a high risk of an attack are also included in the critical areas list for the duration of the event.
3. When an SMS is sent to any mobile located in an area on the critical area list, the SMS center checks the source and destination mobiles to ensure that the SMS is to a mobile and not a control device. A control device most likely doesn't have a message history.
4. The system checks the recipient mobile if it is registered mobile (i.e. the SIM card is registered with the network and has a call log of having generated calls and sent / received SMS messages before.

5. The algorithm also checks to see the frequency of the recipient mobile in that location. If it has been there before, then this condition compared with all the previous conditions have to be met before the messages are delivered but if it is not registered or if it doesn't have a history of delivered messaged or if it is its first time in that location, the message is delayed and analyzed.

The Algorithm checks can be run on any mobile that enters any of the critical areas such that suspicious mobiles are tagged before any SMS is sent to them. Thus mobiles that can receive SMS will be known before the SMS comes and suspicious mobiles phones will not receive any SMS sent to them. This ensures that the Algorithm has no impact on message delivery time. The location of the tagged mobiles can be sent to security forces if the mobiles are found to be stationary beyond the normal operating time of the work area or before the commencement of a major activity within the critical area. It is mandatory in most countries for all mobile numbers to be registered with their operators as such SMS sent to any unregistered mobile phone/ number in the critical area will not be delivered

4.1. Flowchart

The flowchart for the Source Mobile identification and attack prevention algorithm is shown in Figure 7.

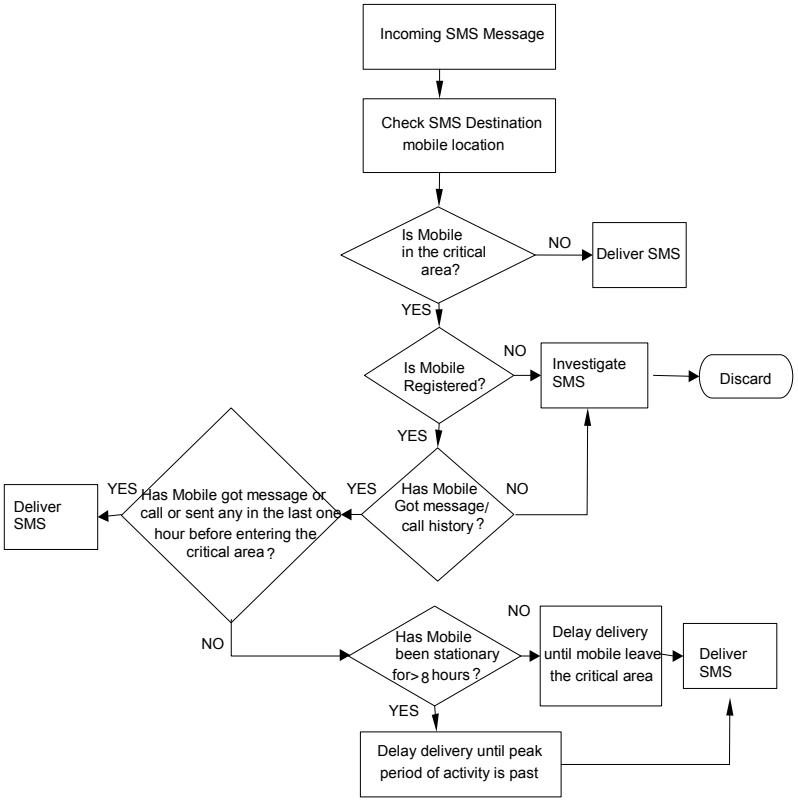

Fig. 7. Flowchart for the Algorithm

4.2. Algorithm for Source Mobile identification

In the event of an SMS triggered explosion, the following algorithm can be used to narrow down and eventually identify the source of the trigger:

1. Isolate all the SMS received by mobiles in the area of the attack
2. Check all the sources of the SMS
3. Check the message history of all the recipient mobile numbers and isolate the mobile without prior receipt or transmitted messages
4. Identify the mobile number that doesn't come on after the attack, it is most likely the trigger module.
5. Identify the source mobiles that communicated with that sent the last SMS to the trigger mobile number and narrow the mobile down to the most frequent registered number on its call log.
6. If the source mobile is an unregistered mobile (and has been probably disposed) track the call logs of that mobile and the cell from where the cell was when the SMS was generated. Video camera feed of the area can be reviewed if they exist.
7. Check all the mobiles that communicated with the source mobile and create a record of the call frequency and duration. The registered mobile can be checked and the identified owners of those mobile can be handed over to the security agencies for further investigative action

5. Conclusion

In the fight against terrorism, there is a constant need to be ahead of the perpetuators of these acts. This work provides an opportunity for governments to take preemptive steps against the period when the terrorists would begin to appreciate the opportunities provided by the use of the GSM platform for the transmission of IED trigger signals. These algorithms will require no change in the network configuration and will introduce minimal impact to the speed of message delivery. The algorithms also provide a means of identifying suspicious GSM modems and SMS trigger enabled IED before the messages are sent. The Early detection of the SMS enabled IEDs will result in a minimization of detonations while ensuring protection of both lives and critical infrastructure.

References

[1] Digital cellular telecommunications system (Phase 2+); Circuit switched voice capacity evolution for GSM/EDGE Radio Access Network (GERAN) (3GPP TR 45.914 version 11.0.0 Release 11) ETSI TR 145 914 V11.0.0 (2012-11) ETSI. 2012
[2] CDMA450 market facts. http://www.cdg.org/resources/files/fact_sheets/CDMA450%20Market%20Facts.pdf Dec 2013
[3] CDMA2000 Market Trends and facts. http://www.cdg.org/resources/files/fact_sheets/CDG_MarketTrendsFacts_English.pdf. December 2013
[4] A.M Zungeru, U.V Edu and A.J Garba. Design and Implementation of Short Message Service based Remote Controller. Computer Engineering and Intelligent systems Vol3 No4 2012
[5] B. Ramamurthy, S.Bhargavi, R. Shashikumar. Development of a low cost GSM SMS-based humidity Remote Monitoring and Control system for Industrial Application. International Journal of Advanced Computer Science and Application. Vol 1 No 4 2010
[6] A.J Al-Mghawish. A practical approach for mobile based remote control. European Scientific Journal June 2013
[7] M.Xu and J.Du. Design of SMS-based remote control system using TC35 and MCU. International Conference on Internet Computing and Information services Hong Kong 2011
[8] V.M Ibrahim, A.A Victor and S.Y Musa. GSM based Anti-theft Security system using AT&T Command. International Journal of Computational Engineering Research. Vol2 Issue 5. 2012
[9] V.Covello, S.Becker, M.Palernchar, Q. Renn and P.Selke. Effective Risk Communication for the Counter Improvised Explosive Devices Threat. Vol 1 US Department of Home land Security Dec 2010
[10] Countering Improvised Explosive Devises. Office of the President of the United States of America Feb 2013
[11] Multi Jurisdiction IED Security Planning guide. US Department of Homeland Security. May 2008
[12] C.W Johnson. A systematic approach for countering the threat to public safety from Improvised Explosive Devices. http://www.dcs.gla.ac.uk/~johnson/papers/ISSC09/IED_2009_v1.pdf
[13] G.D Stevens. Whole of Government Approach to countering Domestic IEDs: Leveraging Military Capabilities. Institute for National Security and Counter Terrorism Syracuse University 2012
[14] K.Wilgucki, R.Urban, G. Baranowski, P.Gradzki, P.Skarzynski. Automated Protection Systems. Military Communications Institute Poland. 2011. http://www.wil.waw.pl/art_prac/2011/Automated_Protection_System.pdf
[15] C.Kopp. Defeating Improvised Explosive Devices. Defense Today Sept 2009. http://www.ausairpower.net/SP/DT-IED-Defeat-Sept-2009.pdf
[16] Remotely Initiated IEDs: GSM Phones and Beyond. Scoping paper. Survey of RCIEDs South East Asia. Feb 2003-Oct 2005. OSS.net http://www.oss.net/dynamaster/file_archive/051011/04e118e543b29b06a494b03a0e192cc8/OSS%2520Remot...